THE NON-REGULAR TRANSITIVE SUBSTITUTION GROUPS WHOSE ORDER IS THE CUBE OF ANY PRIME NUMBER.

By Dr. G. A. Miller, Paris, France.

1. The regular groups of order p^3 (p being any prime number) were published almost simultaneously by Young,* Cole and Glover,† and Hölder.‡ At a considerably earlier date Cayley had published these groups for the special case when $p = 2$.|| It is the object of this paper to determine the remaining transitive groups of this order.

We shall find that there are always two such groups when p is odd. For the special case when p is even it is well known that there is only one.§ Since there are five regular groups of the given order, for every value of p, these facts prove that *the number of the transitive groups of order p^3 is* 6 *or* 7 *as p is even or odd.*

The degree, n, ($n < p^3$) of a non-regular transitive group of order p^3 must evidently satisfy the following conditions:

$$p^3 = an, \quad n! = \beta p^3. \qquad (a, \beta = \text{positive integers})$$

Hence $n = p^2$. Each one of these groups contains a substitution of order p which is commutative to all its substitutions.¶ Since the cycles of this substitution may be regarded as systems of non-primitivity we see that all these groups are non-primitive.**

The degree of the transitive group which corresponds to the permutations of the systems of non-primitivity when one of these groups is transformed by itself is p. Since the order of this group must be a sub-multiple of p^3 as well as of p! the group must be regular. Hence every non-regular transitive group of order p^3 contains a subgroup of order p^2 which does not interchange the systems of non-primitivity.

The problem of constructing all the possible non-regular transitive groups of order p^3 may therefore be divided into the following two parts: 1) The construction of the intransitive groups of order p^2 which may be used as sub-

* American Journal of Mathematics, XV, p. 133.

† Ibid., p. 196.

‡ Mathematische Annalen, XLIII, p. 371.

|| Philosophical Magazine, XVIII, p. 34; cf. ibid., VII, pp. 40, 408.

§ Serret, Liouville's Journal, 1850, p. 52.

¶ Sylow, Mathematische Annalen, V, 588.

** The transitive groups of order p^a are always non-primitive when $a > 1$.

groups, and 2) The construction of the transitive groups of order p^3 which contain these subgroups. We shall consider these parts separately.

2. *The intransitive groups of order p^2 which may be used as subgroups.*

We shall represent the systems of intransitivity of such a group (H) by

$$A_1, A_2, A_3, \ldots, A_p.$$

If one of the substitutions (S) of H would not contain the two systems A_α and A_β ($\alpha, \beta \overline{\gtrless} p$) there would be a transform of S with respect to some substitution in the group of order p^3 which would not contain A_α. Since this transform would contain at least one system (A_γ) which is not found in S, it and S would generate a group of order p^2 whose degree would be less than p^2. All the substitutions of H (excluding identity) must therefore contain either all the systems of intransitivity or all with the exception of one.

The average number of elements in the substitutions of H is $p(p-1)$.* We have just proved that this is also the smallest number of elements that can occur in any substitution of H with the exception of identity. Hence H contains $p-1$ substitutions of degree p^2, $p(p-1)$ of degree $p(p-1)$, and identity.

If we use one of these substitutions (S_1) of degree p^2 as the first generating substitution of H, the cycles of the pth order in a second generating substitution must be the p different powers of the corresponding cycles in S_1. Hence there is one and only one H for each value of p. As this H has been completely determined it remains only to consider the construction of

3. *The transitive groups of order p^3 which contain H.*

If we multiply H by a substitution (S_2) which only interchanges its systems according to a cycle of order p we obtain a group (G_1) which contains only substitutions of the pth order and identity † If we multiply H by sS_2 (s being any cycle of S_1) we obtain another group (G_2) which contains $(p+1)(p-1)$ substitutions of order p and $p^2(p-1)$ of order p^2. It remains to prove that the other groups (G_ϵ; $\epsilon = 3, 4, \ldots$) are not distinct from these two.

Every G is commutative to S_1. We therefore obtain each one of the possible G's once and only once if we multiply H by

$$s_1^{a_1} s_2^{a_2} s_3^{a_3} \ldots s_{p'}^{a_{p'}} S_2, \quad (a_1, a_2, a_3, \ldots, a_{p'} = 1, 2, 3, \ldots, p)$$

where $s_1, s_2, s_3, \ldots, s_{p'}$ are the cycles of S_1, in order, and $p' = p - 2$.

Since

$$(s_1^{x_1} s_2^{x_2} \ldots s_p^{x_p})^{-1} S_2 s_1^{x_1} s_2^{x_2} \ldots s_p^{x_p} = s_1^{x_2 - x_1} s_2^{x_3 - x_2} \ldots s_p^{x_1 - x_p} S_2,$$

* Frobenius, Crelle's Journal, CI, p. 287.

† The only exception occurs when $p = 2$. For this value of p G_1 and G_2 are the same group.

and the system of indeterminate equations

$$x_2 - x_1 = a_1\,, \quad x_3 - x_2 = a_2\,, \quad \ldots, \quad x_1 - x_p = a_p$$

can always be solved when

$$a_1 + a_2 + a_3 + \ldots + a_p = 0\,,$$

all of these groups must be conjugate to

$$Hs_1^{a_1}S_2 \qquad\qquad (a_1 = 1, 2, \ldots, p)$$

with respect to substitutions of the form

$$s_1^{a_1}s_2^{a_2} \ldots s_p^{a_p}\,.$$

When $a_1 = 1$, $Hs_1^{a_1}S_2 = G_2$; when $a_1 = p$, $Hs_1^{a_1}S_2 = G_1$; for the other values of a_1, $Hs_1^{a_1}S_2$ is evidently conjugate to G_2 with respect to the substitutions which transform S_1 into its different powers without interchanging its cycles. Hence G_1 and G_2 are the only non-regular groups of order p^3.

APRIL, 1896.